REMARKS

Claims 14-21 are all the claims pending in the application.

I. Claim Rejections under 35 U.S.C. § 101

Claims 20 and 21 have been rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. In particular, the Examiner has indicated that in order for claims 20 and 21 to be considered statutory, that the claims must be either (1) tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or material) to a different state or thing. In addition, regarding claim 21, the Examiner has indicated that the preamble of this claim must be amended so as to render the claim statutory.

By this amendment, Applicants note that claims 20 and 21 have been amended as suggested by the Examiner in the Office Action. In particular, Applicants note that each of the steps recited in claims 20 and 21 has been tied to the physical structure that is performing the step, and the preamble of claim 21 has been amended so as to be directed to a computer-readable storage medium encoded with a program having computer-executable instructions that when executed by a computer cause the computer to perform the claimed steps.

In view of the foregoing, Applicants respectfully submit that claims 20 and 21 are directed to statutory subject matter, and therefore, kindly request that the above-noted rejection be reconsidered and withdrawn.

II. Claim Rejections under 35 U.S.C. § 112, first paragraph

Claims 14-21 have been rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the enablement requirement.

In particular, regarding claim 14, the Examiner has indicated that features drawn to the "digital signature management unit" and the "control unit" include language that renders claim 14 non-enabling. By this amendment, Applicants note that the above-noted features recited in claim 14 drawn to the "digital signature management unit" and the "control unit" have been modified based on the comments made by the Examiner in the Office Action. In addition, Applicants note that independent claims 20 and 21 have been amended in a similar manner as claim 14.

Accordingly, Applicants respectfully submit that amended claims 14, 20 and 21, as well as dependent claims 15-19, comply with the enablement requirement of 35 U.S.C. 112, first paragraph. Therefore, Applicants kindly request that the above-noted rejection be reconsidered and withdrawn.

III. Claim Rejections under 35 U.S.C. § 112, second paragraph

Claims 14-21 have been rejected under 35 U.S.C. § 112, second paragraph as being indefinite.

In particular, the Examiner has indicated that in claims 14-16, the use of the terms "reading", "generating", and "comparing" renders the claims indefinite, and that in claims 14-16, 20 and 21, that the use of the terms "hold" and "holding" renders the claims indefinite (see items 20 and 21 on pages 10-11 of the Office Action). In addition, the Examiner has indicated that the feature directed to the output of the decrypted content key renders the claims indefinite (see item 22 on page 11 of the Office Action).

By this amendment, Applicants note that the terms "reading", "generating", and "comparing" have been replaced with the terms --read--, --generate--, and --compare--, respectively, and that the terms "hold" and "holding" have been replaced with the terms --store-- and --storing--, respectively. In addition, Applicants note that the claims have been amended so as to clarify the feature directed to the output of the decrypted content key.

In view of the foregoing, Applicants respectfully submit that claims 14-21 satisfy the requirements of 35 U.S.C. 112, second paragraph, and therefore kindly request that the above-noted rejection be reconsidered and withdrawn.

IV. Claim Rejections under 35 U.S.C. § 103(a)

Claims 14-21 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Hori et al. (US 2002/0184154).

Claim 14, as amended, recites the feature of a digital signature management unit configured to (i) generate a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license information stored in the storage unit, generate a hash value of the read encrypted license information, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

Applicants respectfully submit that Hori does not teach or suggest at least the above-noted feature recited in claim 14.

In particular, with respect to Hori, Applicants note that this reference discloses the use of a controller 1420 in a memory card 110, wherein the controller has the ability to generate a hash value, and to encrypt the generated hash value (see paragraph [0223]). In this regard, however, Applicants note that the hash value of Hori is merely a hash value of status information (i.e., information in which a status flag is added to a reception log) (see paragraphs [0219] through [0222]), and therefore, is clearly not a hash value of encrypted license information as recited in claim 14.

In addition, as explained in Hori, a decryption process is performed on the encrypted hash value to obtain a signature data hash corresponding to the encrypted data, and then authenticity of the status information is checked based on the encrypted status and the signature data (see paragraph [0027]). Thus, while Hori discloses the ability to determine the authenticity of the status information based on the encrypted status information and the signature data, Applicants respectfully submit that this aspect of Hori clearly does not correspond to the feature recited in amended claim 14 which indicates that the hash value stored in the built-in memory is compared with the generated hash value of the read encrypted license information.

Based on the foregoing, Applicants note that while Hori discloses the ability to generate a hash value of status information, and to determine the authenticity of the status information based on the encrypted status information and the signature data, that Hori does not disclose or in any way suggest the above-noted feature recited in claim 14 of a digital signature management unit configured to (i) generate a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and store the generated hash value into a built-in memory, and (ii) read the encrypted license information stored in the storage unit, generate a hash value of the read encrypted license information, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

Accordingly, Applicants respectfully submit that amended claim 14 is patentable over Hori, an indication of which is kindly requested.

Regarding claims 15-19, Applicants note that these claims depend from claim 14 and are therefore considered patentable at least by virtue of their dependency.

In addition, regarding claim 16, Applicants note that this claim has been amended to recite that the digital signature management unit is configured to (i) generate a hash value of the encrypted correspondence table before the encrypted correspondence table is stored into the storage unit, and store the generated hash value into the built-in memory, and (ii) read the encrypted correspondence table stored in the storage unit, generate a hash value of the read encrypted correspondence table, and compare the hash value stored in the built-in memory with the generated hash value of the read encrypted correspondence table, with a result of the comparison being used to verify validity of the read encrypted correspondence table, the validity indicating that the read encrypted correspondence table has not been tampered with.

Regarding the above-noted feature, Applicants note that the Examiner has recognized that Hori does not disclose or suggest such a feature, but has taken the position that it would have been obvious to encrypt a correspondence table and store the result in a storage unit "for the purpose of providing a data distribution system" (see Office Action at page 14).

With respect to the Examiner's above-noted position, Applicants note that as explained in MPEP 2142, in view of the decision in *KSR International v Teleflex Inc.*, there must be a "clear articulation of the reason(s) why the claimed invention would have been obvious" (emphasis added). Further, MPEP 2142 also indicates that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" (emphasis added).

In the present case, Applicants submit that the above-noted statement by the Examiner indicating that it would have been obvious to modify Hori to provide the above-noted feature recited in claim 16 "for the purpose of providing a data distribution system" is not a clear articulation of the reason why one of ordinary skill in the art would have modified Hori in the manner suggested by the Examiner, and is not an articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. Instead, Applicants note that this statement by the Examiner is merely conclusory, and includes absolutely no factual basis as to why one of ordinary skill in the art would have modified Hori so as to provide the above-noted feature recited in claim 16.

For example, Applicants note that Hori is directed to a data distribution system using a memory card (e.g., see the title of Hori and paragraph [0001]). As such, regarding the Examiner's statement that it would have been obvious to modify Hori so as to include the above-noted feature recited in claim 16 "for the purpose of providing a data distribution system", Applicants respectfully submit that this statement is clearly conclusory, and is in no way whatsoever an articulation of a reason why one of ordinary skill in the art would have modified Hori in the manner suggested by the Examiner.

Further, Applicants note that the Examiner has not addressed the above-noted feature recited in claim 16 directed to the comparison of the hash value stored in the built-in memory with the generated hash value of the read encrypted correspondence table. Applicants respectfully submit that Hori clearly does not disclose or suggest such a feature, and that it would not have been obvious to one of ordinary skill in the art to modify Hori so as to include such a feature.

In view of the foregoing, Applicants respectfully submit that Hori does not disclose, suggest or render obvious all of the features recited in claim 16. Accordingly, Applicants submit that claim 16 is patentable over Hori, an indication of which is kindly requested.

Regarding claims 20 and 21, Applicants note that each of these claims has been amended in a similar manner as claim 14 so as to recite the feature of a digital signature management step, being performed by the digital signature management unit, of (i) generating a hash value of the encrypted license information before the encrypted license information is stored into the storage unit, and storing the generated hash value into a built-in memory, (ii) reading the encrypted license information stored in the storage unit, generating a hash value of the read encrypted license information, and comparing the hash value stored in the built-in memory with the generated hash value of the read encrypted license information, with a result of the comparison being used to verify validity of the read encrypted license information, the validity indicating that the read encrypted license information has not been tampered with.

For at least similar reasons as discussed above with respect to claim 14, Applicants respectfully submit that Hori does not disclose, suggest or otherwise render obvious the above-noted feature recited in claims 20 and 21. Accordingly, Applicants submit that claims 20 and 21 are patentable over Hori, an indication of which is kindly requested.

V. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Motoji OHMORI et al.

/Kenneth W. Fields/
By 2009.11.30 14:46:58 -05'00'
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/krg
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
November 30, 2009